REMARKS

Claims 4, 6-7 and 35-51 are pending. Claims 4, 7 and 39 are the independent claims.

I. Office Action Summary

In the Office Action dated July 7, 2009, the Examiner has rejected the claims as failing to comply with the written description requirement under 35 U.S.C. § 112, paragraph 1. The examiner has withdrawn the prior rejection under 35 U.S.C. § 103 and has substituted a new § 103 rejection. In this Office Action, all the pending claims (4, 6-7 and 35-51) are now rejected as obvious over the combination of Hirota et al. (U.S. 6,856,431) in view of Japanese reference JP 11250141.

II. Rejections Under 35 U.S.C. § 112, 1st paragraph

The office action suggests that the specification only supports portions of tracks being decrypted rather than portions of files. Applicants submit that support for the current claim language is expressly provided.

Applicants note that the specification expressly supports that portions of files are decrypted. Referring to FIG. 3C, a track is made up of one or more files (shown as AOBs or "audio objects"). Each AOB is made up of AOB blocks 312, each AOB block is made up of AOB elements 316 and each AOB element is made up of one or more AOB frames 320. As noted in paragraph 0039 of the specification, each two seconds of playback may comprise a variable number of frames. Referring to paragraph 0092, the specification recites that a portion of a track is played back and that "this portion may be ***in*** any of the files that comprise the track." (emphasis added). Paragraph 0092 continues by noting that "the portion may be anywhere from a fraction of a second . . . to about ten seconds" and is preferably two seconds. Thus, the language in the current claims regarding retrieving and decrypting a portion of a file is expressly supported by the specification. Withdrawal of the §112 rejection is respectfully solicited.

III. Rejections Under 35 U.S.C. § 103(a)

Applicants respectfully disagree with the Examiner's rejection the claims over Hirota et al. (previously applied) and JP 11250141(newly applied).

CLAIM 4

Independent claim 4 recites a device for playback of encrypted audio and/or video tracks from a memory card. The device comprises:

> a processor; and
>
> a module operatively coupled with the processor and configured, for each audio and/or video file within an audio and/or video track, for:
>
> > obtaining an encrypted key from a protected area of the memory card;
> >
> > retrieving only a portion of the audio and/or video file from the memory card;
> >
> > decrypting the obtained encrypted key;
> >
> > decrypting the portion of the audio and/or video file with the decrypted key; and
> >
> > deleting the decrypted key after decrypting the portion of the audio and/or video file before decrypting an additional portion of the file.

Claim 4 recites a module that is configured for each audio and/or video file comprising an audio and/or video track to retrieve only a portion of the audio and/or video file, decrypt the portion of the file and delete the decrypted key before decrypting an additional portion of the file of the track.

Applicant reiterates the deficiencies of Hirota, for example its lack of any teaching or suggestion of deleting a key as claimed. Hirota teaches a playback apparatus that plays tracks of audio made up of one or more encrypted files referred to as audio object (AOB) files. Each AOB file has a unique filename and has a "File Key" for decrypting the respective AOB file that has a name that substantially matches the name of the AOB file (Col. 10, lines 18-30; FIG. 9, Col. 13, lines 22-57). When an encrypted AOB file in Hirota is played back, the appropriate FileKey is retrieved and placed in RAM in a FileKey Storing Area 14 and the FileKey and is sent to descrambler 7 (FIG. 52; Col. 43, lines 1-6; Col. 44, lines 37-48). The FileKey is maintained in the descrambler while the entire AOB file is decrypted and played back (See Col. 47, lines 21-27). Hirota is completely missing at least the element of a module configured for "deleting the decrypted key after decrypting the portion of the audio and/or video file before decrypting an additional portion of the file".

Thus rather than teaching or suggesting the device of claim 4, where only a portion of the file is retrieved, a key is decrypted, the retrieved portion is decrypted with the decrypted key and then the key is deleted before decrypting another portion of the file, Hirota keeps the key in a descrambler until the file is decrypted. Claim 4 defines tracks having one or more files and a device for playback having a module configured for deleting a decrypted key after decrypting a portion of the file. As noted in the present disclosure, an advantage of only decrypting only a portion of a file and deleting the key each time a portion has been decrypted before going on to decrypt another portion is that the amount of decrypted file is kept small and the key is only in a decrypted state for a very short time. In contrast Hirota discusses how it attempts to minimize the damage that exposing a FileKey will cause by using a separate FileKey for each AOB file, rather than a portion of a file, but that the key is left in the descrambler for the entire time a file is being decrypted.

Applicants note that the present office action now replaces the previously cited Dolan reference with the newly cited JP 11250141 reference as allegedly disclosing the step of deleting the decrypted key before decrypting an additional portion of the file that is missing from Hirota. However, Applicants note that JP11250141 also lacks this feature.

Applicants have obtained a machine translation of JP 11250141, copy attached, and presume that the Examiner has done the same since Applicants only possessed and submitted a translated abstract previously. If the Examiner's translation differs from the attached, Applicants respectfully request that the

Examiner provide Applicants with a copy of the translation the Examiner is relying on.

Careful review of the machine translated JP 11250141 and the paragraphs cited by the Examiner show that a decryption key is maintained in memory until all of the contents to be decrypted have been downloaded and decrypted. For example, paragraphs 0021-0025 of JP 11250141 recite:

> [0021]***The decode key deleting means 7 is deleted after decoding, reproduction, and deletion to all the data of corresponding contents end the decode key acquired by the decode key acquisition means 5.***
> [0022]In said composition, if a user orders reproduction of a certain (enciphered) contents in the terminal 2, the decode key acquisition means 5 will start and the message a which specifies which key of which key center the decode key corresponding to said contents is will be sent to the computer network 3. The key center 1 which received the message a via the computer network 3 returns the message b containing a corresponding decode key.
> [0023]The decode key acquisition means 5 of the terminal 2 which received the message b via the computer network 3 takes out a decode key from this message b, and sends it to contents decoding, reproduction, and the deleting means 6.
> [0024]Contents decoding, reproduction, and the deleting means 6 read a constant rate of first data from the enciphered contents, performs decoding and reproduction using said decode key, and deletes the this decoded data. Next, a constant rate of data following said read data is read, and said same processing is performed. A fixed quantity of data in the enciphered contents is read every like the following, and decoding, reproduction, and deletion are repeated.
> [0025]Thus, ***after decoding, reproduction, and deletion to all the data of contents are completed, the decode key deleting means 7 deletes a decode key.***
>
> (emphasis added)

This section, and the remainder of JP 11250141, appears to disclose a system where a key is read and then used to decrypt all data for a file, where the data is downloaded at a constant rate. The data are deleted at regular intervals (see discussion on contents decoding, reproduction and a deleting means – item 6 in drawing 2), but the key is only deleted after all of the content (i.e. all read operations) for a file are completed (see discussion on decode key deleting means – item 7 in drawing 2). JP11250141 fails to teach or suggest at least the step of "deleting the decrypted key after decrypting the portion of the audio and/or video file before decrypting an additional portion of the file" as claimed in claim 4.

Accordingly, Applicants respectfully submit that claim 4 distinguishes over Dolan and JP11250141, alone or in combination for at least the above reasons. Claims 6 and 35-38 are dependent claims, therefore their allowability directly follows from the allowability of independent claim 4.

CLAIM 7

Claim 7 relates to a computer readable storage medium having an executable program configured to, for each encrypted audio or video file comprising an encrypted track:

> decrypt an encrypted audio or video file from the memory card,
>
> wherein decrypting the audio or video file comprises:
>
> (a) decrypting a key stored in the memory of the device;
>
> (b) decrypting a portion of the audio or video file less than an entirety of the audio or video file;
>
> (c) deleting the decrypted key; and
>
> (d) repeating (a) through (c) until the entirety of the audio or video file is decrypted.

Although of different scope than claim 4, claim 7 also recites the feature of deleting a decrypted key after each portion of a file is decrypted. Again, this is different than the teachings or suggestions found in Hirota, where a decrypted key is left in a descrambler for the decryption of an entire file, or JP11250141, which only discloses deleting a key after encrypting an entire message.

Accordingly, for at least these reasons, Applicants submit that claim 7 is allowable over the cited art.

CLAIM 39

Claim 39 recites a method for playback of audio and/or video tracks comprising one or more encrypted audio and/or video files stored on a memory, where the method includes:

> obtaining an encrypted key from a protected area of the memory card with a device having a processor and a memory operatively connected with the processor;
>
> retrieving only a portion of an audio and/or video file from the memory card with the device, wherein the audio and/or video file comprises at least a portion of an audio and/or video track;
>
> decrypting the encrypted key;
>
> decrypting the portion of the audio and/or video file with the decrypted key; and
>
> deleting the decrypted key from the device after decrypting the portion of the audio and/or video file before decrypting an additional portion of the audio and/or video file.

Although of different scope than claims 4 and 7, claim 39 recites steps relating to deleting a decrypted key after each portion of a track is decrypted and before the next portion of the file is decrypted. Accordingly for at least the same reasons as noted for claims 4 and 7, Applicants submit that claim 39 is allowable over the cited art. Claims 40-51 are dependent claims. Accordingly, their allowability directly follows from the allowability of independent claim 39.

III. Conclusion

In light of the above remarks, Applicants submit that claims 4, 6-7 and 35-51 are in condition for allowance. A Notice of Allowance is respectfully requested.

Respectfully submitted,

Kent E. Genin
Registration No. 37,834
Attorney for Applicants

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200